Weeks of debugging can save you hours of TLA$^+$

Markus A. Kuppe

Engineer@Microsoft

TLA$^+$ 30.000ft above

TLA$^+$ is a specification language to design, document, and verify reactive systems.

Figure: TLA+ creator

TLA$^+$ 30.000ft above

TLA$^+$ is a specification language to design, document, and verify reactive systems.

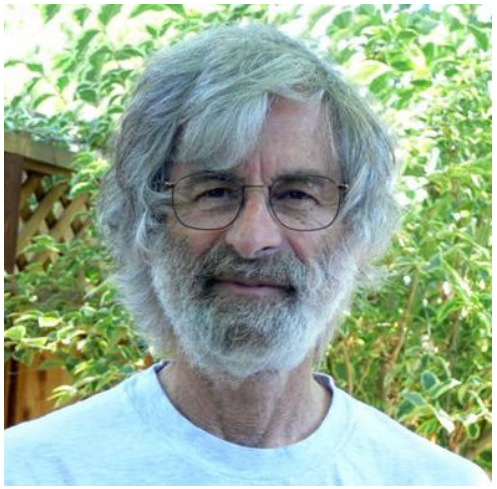

Figure: Leslie Lamport

A few days ago...

Bounded MPMC Queue

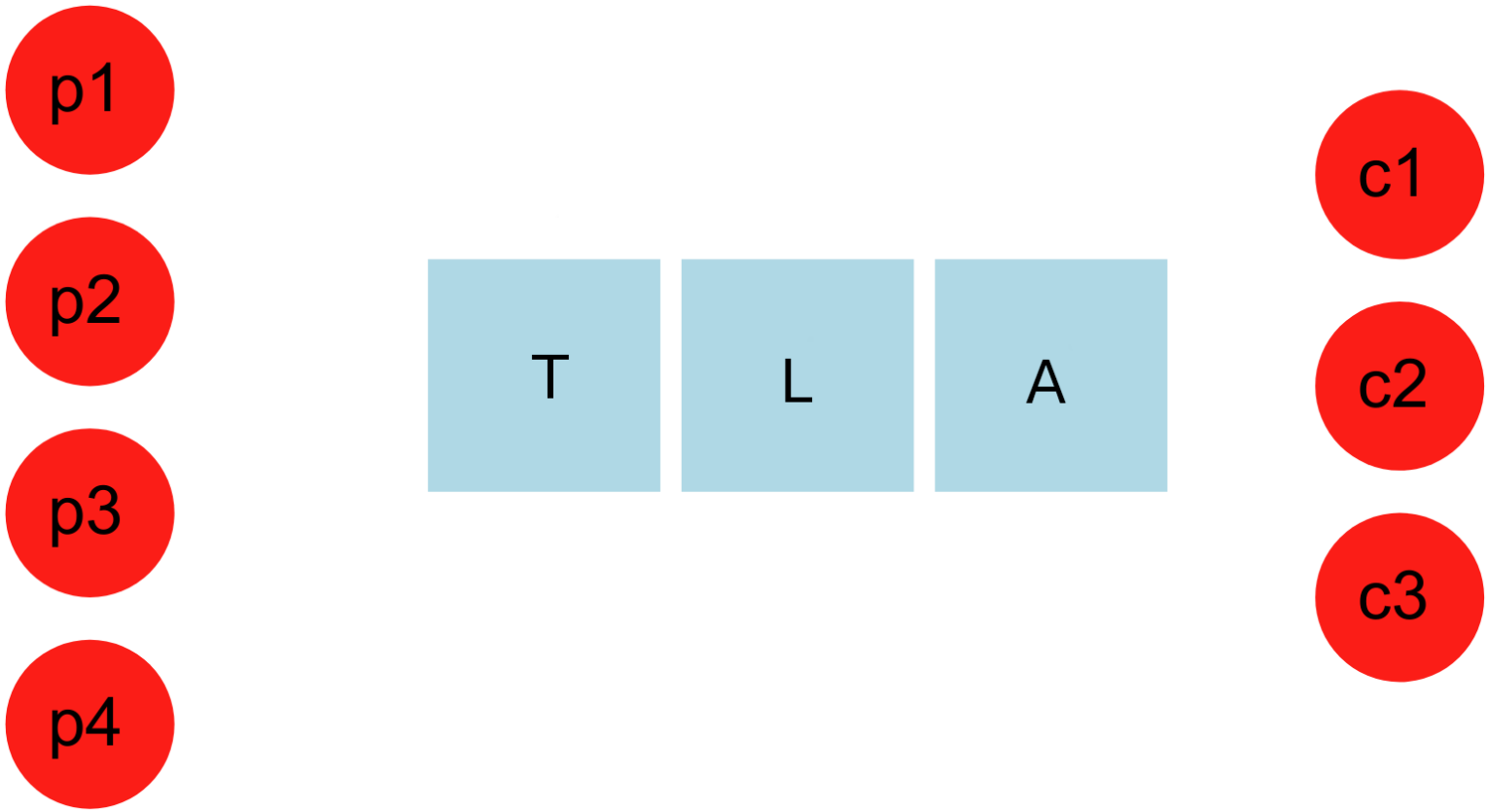

Figure: Deadlock!!!

A few weeks later...

A few weeks later...

Wrap-up

- Developed a spec for the bounded MPMC queue
  - Reproduced:
    - Deadlock (safety)
    - Starvation (liveness)
  - Verified fixes for both issues
  - ...for three, small configurations
  - => Small-Scope Hypothesis
- TLA proof system for stronger guarantees
  - Beware: proofs usually too expensive
- Implementation of specs

=> Walkthrough Tutorial: `https://aka.ms/tlabq`

Summary

- Disclaimer:
  - Verification does not replace testing but supplement it
  - Spec langs do not replace programming languages but supplement them
- Why specs are useful for SRE (postmortems)?:
  - self-contained
  - human-readable & math is the lingua franca of engineering
  - high-level
- Math (TLA$^+$) is easy-ish to learn
  - Lamport's Video Course: `https://aka.ms/tla`

Q&A

Q&A